WHAT IS CLAIMED IS

1. A method for detecting malicious code in a stream of data traffic input to a gateway of a data network, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in the stream of data traffic;

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled code;

wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction; and

(d) accumulating said threat weight to produce an accumulated threat weight.

2. The method, according to claim 1, wherein said at least one suspicious portion of data contains at least one illegal character in a protocol of the stream of data traffic.

3. The method, according to claim 1, wherein said monitoring is performed by skipping acceptable data in the stream of data traffic, said acceptable data being consistent with a protocol used by the data stream.

4. The method, according to claim 3, wherein said acceptable data includes acceptable executable code.

5. The method, according to claim 1, wherein upon reaching a branch in said disassembled code, further accumulating said threat weight respectively for each branch option in said disassembled code, thereby producing said accumulated threat weight for each said branch option.

6. The method, according to claim 1, further comprising the step of

(e) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of

(i) generating an alert, and

(ii) blocking traffic from the source of the suspicious data.

7. The method, according to claim 6, wherein said blocking is solely in the stream of data traffic.

8. The method, according to claim 1, wherein said attempting to disassemble is initiated at a plurality of initial instructions, each of said initial instructions with a different offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset.

9. The method, according to claim 1, wherein said attempting to disassemble is initiated at an initial instruction of an address of previously known offset relative to a vulnerable return address.

10. The method, according to claim 1, wherein the stream of data traffic includes an encoded data portion, further comprising the step of, prior to said attempting to disassemble:

(e) decoding said encoded data portion.

11. A method for detecting malicious code in a stream of data traffic input to a gateway of a data network, the stream of data traffic including data packets, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in the stream of data traffic;

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said suspicious data thereby attempting to produce disassembled code;

wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction; and

(d) accumulating said threat weight to produce an accumulated threat weight;

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction, and

(ii) decreased for an illegal instruction.

12. The method, according to claim 11, wherein said attempting to disassemble is initiated at a plurality of initial instructions, each of said initial instructions with a different offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset.

13. The method, according to claim 11, wherein said attempting to disassemble is initiated at an initial instruction of an address of previously known offset relative to a vulnerable return address.

14. The method, according to claim 11, further comprising the steps of:

(e) receiving the data packets input from a wide area network interface of the gateway, thereby building the packets into a virtual stream inside the gateway; and

(f) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of

(i) generating an alert, and

(ii) blocking traffic from the source of the malicious code.

15. A stream of data traffic purged of malicious code, according to a method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in the stream of data traffic;

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said suspicious data thereby attempting to produce disassembled code;

wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction;

(d) accumulating said threat weight to produce an accumulated threat weight

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction, and

(ii) decreased for an illegal instruction;

wherein upon said accumulated threat weight exceeding a previously defined threshold level; and

(e) blocking traffic from the source of the malicious code.

16. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for detecting malicious code in a stream of data traffic in a data network, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in the stream of data traffic;

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said suspicious data thereby attempting to produce disassembled code;

wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction; and

(d) accumulating said threat weight to produce an accumulated threat weight;

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction, and

(ii) decreased for an illegal instruction.

17. A computer system comprising,

(a) a processor;

(b) a program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for detecting malicious code in a stream of data traffic in a data network, the method including the steps of:

(A) monitoring by the system for at least one suspicious portion of data in the stream of data traffic;

(B) upon detecting said at least one suspicious portion of data, attempting to disassemble said suspicious data thereby attempting to produce disassembled code;

wherein for each instruction in said disassembled code,

(C) assigning respectively a threat weight for each said instruction; and

(D) accumulating said threat weight to produce an accumulated threat weight;

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction, and

(ii) decreased for an illegal instruction.

18. The method, according to claim 17, wherein said attempting to disassemble is initiated at a plurality of initial instructions, each of said initial instructions with a different offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset.

19. The method, according to claim 17, wherein said attempting to disassemble is initiated at an initial instruction of an address of previously known offset relative to a vulnerable return address.

20. An apparatus for detecting malicious code in a stream of data traffic input to a gateway to data network, the apparatus comprising:

(a) a filter apparatus which filters and thereby detects at least one suspicious portion of data in the stream of data traffic;

(b) a disassembler attempting to convert binary operation codes into assembly instructions of said at least one suspicious portion of data, thereby attempting to produce disassembled code; and

(c) an assembly instructions analyzer which for each of said instructions assigns respectively a threat weight, accumulates respectively said threat weight, thereby produces an accumulated threat weight.

21. The apparatus, according to claim 20,

wherein said attempting to convert is initiated at a plurality of initial instructions, each of said initial instructions with a different offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset.

22. The apparatus, according to claim 20, further comprising:

(d) a vulnerable return address detector which detects an initial instruction for said attempting to convert.